Volume 17, Issue 27 Atari Online News, Etc. July 24, 2015

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1727 07/24/15

~ AshleyMadison Is Hacked ~ Twitter Safety Center! ~ Win 10 Auto Update!

-* Right To Be Forgotten in US? *-
-* Bogus Twitter Buyout Story Stock Hit *-
-* Microsoft Rushes Emergency Win Security Fix *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""

Can you believe that we’re almost to the end of July already? After this past long and horrific winter, one would hope that Spring and Summer would hang around, but they both flew by! I had better start enjoying it more before it’s gone!

Lots of interesting stuff for you again this week, including a number of Atari-related tidbits - including another installment from Fred Horvat on his ongoing experiences with his new Firebee. We hope that you enjoy it and everything else this week!

Until next time...

=~=~=~=

## Experimenting With The Firebee

by Fred Horvat

At the end of my last submission to AONE I was discussing building my own Aranym MiNT setup and not having any luck with getting NVDI 5 installed and running. Unfortunately since finding a solution I have not sat down to attempt the installation. Mostly because of not being quite sure if the Araynm build I was planning on using was clean anymore. I most likely changed settings and added programs to test. I would have to start from scratch with EasyMiNT again. Not horrible but I didn t spend the time to start over yet.

During this time I started looking into running Atari programs and MiNT on real hardware again. During this time I also sold my Atari Falcon30 and TT030. I still have a TT030 left with 4ST and 16TT Ram installed. I brought it out of storage and found out it had no hard drive inside of it anymore. More searching for an external hard drive to use or a SCSI 1 hard drive to put inside. I found an external hard drive and attached it to the TT. Turned both on and to my surprise it had a fresh install NAES 2.0 on it. Everything was still in German so I knew it was a fresh install. Via floppy I installed Teradesk in English and changed the config files to load Teradesk instead of the German Thing Desktop. NAES 2.0 has the version of MiNT 15.5 as part of the installation. This is an old version of MiNT as the current version is 1.19. It works fine so for the time being this was not an issue and I could pretty easy upgrade MiNT to a more current version. Next step was that I wanted Ethernet for the TT. I did some searching and saw that many of the cartridge port Ethernet Cards for the Atari computers are no long being built. I did track down some used ones though. There are other options available also like specific SCSI to Ethernet adapters and using the Serial Port with a Null Modem cable to either a Linux or Windows PC. I looked into the Serial Port solution at https://sites.google.com/site/probehouse/networking-the-atari/using-ppp-win7 If doing this method I would most likely choose a Windows PC to use over Linux as I have more Windows PC available than Linux. Before doing anything I thought about using the TT and decided against it for these reasons: The TT Medium Resolution (640x480x16 colors) looks really bad on all the LCD monitors I own. It only looks good on a real CRT monitor as the TT has slightly different refresh rates of the standard VGA standard. Also I want to use whatever machine on my 4-Port USB KVM. A KVM is a device that in my case can use up to 4 computers attached to a single USB keyboard, single USB mouse and a single 15 Pin VGA plug monitor. The standard TT cannot attach to the USB KVM. Lastly I would also need a Windows PC running at the same time to use Ethernet, assuming I did get this working in the first place.

Now I started thinking about looking into an Atari Clone. I heard for almost 10 years now about the Atari Coldfire Project (ACP) that eventually lead to the FireBee computer. I didn t follow very closely the progression of the project but through the Usenet, A-ONE, Tuesday Night Chats on Atarinews.org, and others I am in contact in the Atari Community I knew just enough about the project. So I sat down and started searching on the Web for more information about this machine. Much to my surprise this was not the only Atari Clone currently available! There are a couple of FPGA machines available. What the FPGA allows you to do is via firmware/software change what the computer is. In this case turn the board into an Atari ST Computer. If you want to boot Amiga OS change the firmware and you can boot it as an Amiga and much more. More information about FPGA chips can be found here: https://en.wikipedia.org/wiki/Field-programmable_gate_array. First Atari Clone I looked at was the the Suska FPGA machine http://shop.inventronik.de/store. This unit looked very promising with all the attachments available. Unfortunately what kept me from researching much further was the starting price 619.00 Euros plus whatever attachment I wanted plus shipping and insurance from Germany to the USA. The next FPGA unit I saw was the MIST. http://lotharek.pl/product.php?pid=96  This unit starts out at 199.00 Euros. I did more research on this unit and saw that it was a very good Atari Clone that ran many games though this is not what I wanted it for it lead me to believe that the developer had it running very good if games played well on it. I saw that you could attach certain branded USB to Ethernet adapters to it for networking. This was what I was looking for. Before purchasing a unit though I decided to install MiNT under Hatari with 14MB RAM and a 68000 CPU since this is what an ST is capable of. I still have NAES 2.0 CD so I installed NAES under Hatari and used it for a while with software I wanted to use without Networking because Hatari is not capable of that. Limitations I saw where 14MB of RAM though for what I was running worked fine under MiNT. The 68000 CPU this is was my biggest concern. A lot of newer software requires a 68030 and FPU. Then lastly was the Atari ST High Resolution Mode of 640x400x2 colors (Black and White). From what I read about the MIST board was that it is not just limited to 8mhz but it is running a 68000 CPU and it was not obvious on their Web Site about running higher than standard Atari ST resolutions. Then something I didn t consider initially was the Raspberry Pi computer.

https://en.wikipedia.org/wiki/Raspberry_Pi and https://www.raspberrypi.org/ What made me think about this was that a coworker had recently purchased the updated Raspberry Pi 2 unit for a media server and her had some Unix questions. A local retailer where I live Microcenter http://www.microcenter.com/ is big into Raspberry Pi and other electronic project parts and kits. I did a little research and saw that the Raspberry Pi ran Aranym and Hatari. This is not exactly what I was looking for because it would be running basically emulators (Aranym and Hatari) but it would be a separate machine that is small and easily portable. I decided to take the plunge and get a unit. For $80US I purchased a Raspberry Pi 2 board, a clear case to put it in, HDMI to VGA adapter, and two 8GB Micro SD cards. I used a Micro USB power adapter from an old Cell Phone to power the unit. Once I had the unit I put it all together and went through the steps on downloading and installing Linux to one of the SD Cards. Once running Linux I installed Aranym and Hatari and copied over my working Aranym builds I had like AFROS, EasyARAMiNT, and my own and my Hatari MiNT build I did for testing. Much to my disappointment networking did not work under Aranym. This is a show stopper for me. I did some searching on the Web and did not find a solution for this with the Raspberry Pi. Aranym is very fussy with TCP/IP and I have it working only on my PPC and Intel Macs. No one I heard read online has gotten it work under Windows and people have had better luck under some Linux s. Then Hatari could not read any hard drive or floppy image that I copied to the SD card or downloaded. I could create floppy and hard drive images and put on whatever I wanted but I could not use any existing floppy or hard drive images. So to use Hatari I would have to create everything from scratch that I wanted to use. Not totally horrible but without Networking it isn t worth my effort. I checked the versions of Aranym and Hatari for the Raspberry Pi and they are 3-4 years old which could be the whole issue. I could always attempt to compile the latest versions and hope for the best assuming I could get them to compile. I ve tried a couple of times with help on http://www.atari-forum.com/index.php to get the latest Aranym to compile under FreeBSD but I have not had any luck with that yet. I am not a C developer and haven t done any C coding in about 15 years so that s just not my area of expertise.

To be continued

## Cho Ren Sha 68k for the Atari Falcon030

Here’s the first beta release of Cho Ren Sha 68k for the Atari Falcon030.

Requirements:  
Atari Falcon030 with 14 MB RAM.  
Supports:  
Jaguar Pad/Power Pad.  
TV/RGB and VGA.  
Features:  
DSP assisted sprite engine.  
Up to 65536 colours.  
Gameplay recording and replay.  
Highscore saving.

Notes:

The first beta does not support accelerated machines.

Scrolling will be added later.
No in game music.
Should work with an accelerator which guarantees the synchronisation between CPU and DSP (Nemesis, Phantom, Skunk(?), ...).
Use the arrow keys and the LEFT SHIFT and CONTROL keys if you don’t have a joystick attached.
Sample replay seems to have some problems within the menu.
Known issues so far:
Please use a "non ST compatible" screen mode before starting the game to avoid a garbled display after exiting the game.
Needs an original TOS version (like TOS 4.02) due to the usage of the DSP interface.
Be careful with the "in game settings" to prevent a game freeze.
Please note that there’s a special binary for the Hatari emulator (older versions) in case you’re having display problems.

Download it here: Cho Ren Sha 68k for the Atari Falcon030 (Beta 1)
http://www.atomic-skulls.de/temp/crs_b1.zip

Some video impressions (taken from the "X68000 porting" thread):
"Bullet Hell"
https://www.youtube.com/watch?v=87EMhNkTkeo

"Insanity"

https://www.youtube.com/watch?v=voiRnr72YhQ

Have fun!

## Ask LH: Are These Old Atari Chips Worth Anything?

Dear Lifehacker, I have a collection of chips belonging to old Atari game carts. (Photo attached.) My dad s friend used to work for Atari as a developer of Atari games and he gave these chips to us. Do you know if it is worth anything? I have 11 games. Thanks, Nova

Hi Nova,

As the old adage goes, a product is worth what someone s willing to pay for it. The trick is finding those who are willing to pay.

There s less of an overall market for retro Atari stuff compared to, say, Nintendo rarities, but that very much depends on what you ve actually got.

There s not that much to go on from the supplied image   I m guessing they re Atari 2600 internals, but Atari did dabble in cartridges for their other computer formats as well. If it s for the 400/800 series, for example, they re probably worth a whole lot less, simply because there s far fewer rabid collectors for that particular set of systems.

Realistically, you re looking at value from two different sources, one of which is arguably going to be far more lucrative than the other. There s the collector set that enjoys having the physical object, especially if it has rarity. These are the mobs who tend to display rather than play, and would most likely buy your chips to encase in a box as a trophy somewhere.

However, that s very much conditional on what s actually on the chips. This is where the real potential value lies. If what you ve got, is, say, Atari 2600 Pac-Man, an incredibly common cart, then you re sitting on almost no value at all, unless you could somehow prove they came in prototype form from Atari itself.

If, however, you re sitting on rare software, or even better an unreleased game, then there s potential for them to be worth quite a bit more, depending on what you have.

Were I you, I d chase down this friend of your Dad s and see if he s still got something that can read the content of the chips to determine what actual software, if any, is present. It s most likely that they wouldn t run on a straight production machine, and I d be wary of automatically trying that, because a fried chip isn t going to be worth anything.

If it s a previously unknown game it could be worth thousands, but if it s common, or the chips haven t actually been burnt with any actual software, then they re not going to be worth much at all. If it s a game that s still regarded as rare, and you can back up the provenance of where it s from, you could be looking at a decent little sum of money. But the first step has to be working out what s actually on those chips.

=~=~=~=

->In This Week’s Gaming Section  - Pete Kauffman Passes Away!
  """""""""""""""""""""""""""""

=~=~=~=

->A-ONE’s Game Console Industry News   -  The Latest Gaming News!
  """"""""""""""""""""""""""""""""""

Pete Kauffman Passes Away

News has broken that the video game industry has lost another pioneer, Exidy founder Pete Kauffman. Exidy may not be well-remembered by most gamers anymore as they went bankrupt and exited the video game market in the mid-80s. The attempt to break out into the home console market also didn t work out very well. But they were influential during the golden age of gaming, producing a number of great games in their time on the market. Some of those were notable for various reasons: Death Race began the debate about violent games; Car Polo had full color graphics in 1977 (not a first but it was still quite rare to come across at the time); Star Fire had the first cockpit cabinet; Venture brought adventure gaming to the arcade; Crossbow innovated the light-gun space and so on.

There is a brief obituary for Mr. Kauffman at Gamasutra; RIP Pete.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

## Do Americans Have The Same Right As Europeans To Be "Forgotten" by Google?

Europeans have the right to request the removal of links in search engine results - what is now commonly referred to as the "right to be forgotten," thanks to a May 2014 court ruling.

Should Americans also have the right to be forgotten?

According to Consumer Watchdog, a nonprofit advocacy organization, the answer is "yes" - and the group wants the US Federal Trade Commission (FTC) to do something about it.

In a complaint filed this week with the FTC, Consumer Watchdog says Google has an obligation to protect US consumers’ privacy rights by extending the ability to request the removal of links from Google search results to Americans.

Since the ruling last year by the European Court of Justice requiring Google (and other search engines such as Bing) to take down links that are no longer "relevant," Google has reluctantly obliged with a request form available in European countries.

As of this morning, there had been 282,001 total requests so far to remove more than 1 million URLs. Google has taken down 41% of those URLs.

But Consumer Watchdog claims that Google is engaging in "unfair" and "deceptive" practices by not giving Americans the same ability to request link removals.

The FTC’s mandate, under the Federal Trade Commission Act, is to protect US consumers from unfair or deceptive practices in commerce.

In recent years, the FTC has evolved from an agency mainly concerned with anti-trust issues into the US government’s primary regulator of privacy issues raised by emerging communications and financial technologies.

According to Consumer Watchdog’s complaint, because Google does not offer Americans "a key privacy tool," Google is engaging in deceptive practices by "aggressively and repeatedly" making claims to protect users’ privacy, such as those in its statement of privacy principles.

The group’s complaint also says Google is engaging in unfair practices because not offering the right to be forgotten causes "substantial injury" to US consumers.

As examples of the harm caused, Consumer Watchdog cites cases where links showing up in search results for a person’s name have led to job losses or emotional distress:

A school guidance counselor was fired when photos of her posing as a lingerie model were found online and shown to the school principal. Mugshot photos of a woman who was arrested and charged with domestic violence after being attacked by her boyfriend show up among the top search results for her name, even though the charges were later dropped. Grisly photos of a young woman decapitated in an accident show up when her name is searched, causing harm to her parents.

Interestingly, the above cases all involve photos - Google frequently removes images from search results that are protected under copyright, and recently announced it will grant takedown requests for "revenge porn" images.

Google also removes other kinds of information from search results, such as national identification numbers (like US Social Security numbers), bank account numbers and credit card numbers.

Under the European court ruling, search engines do not have to remove links to information that serves the public interest, such as news articles about public figures.

Google might have a hard time leaning on the First Amendment, or claiming that its search algorithms are impartial, as reasons not to grant the right to be forgotten to Americans.

What do you think, readers? Should Americans, and everyone else outside of Europe, also have the right to be forgotten?

Is control over what information shows up in search results a privacy right? Does removing links to content count as censorship?

## Twitter s Safety Center Teaches Users How to Deal With Abuse

To curb abuse on its site, Twitter can t just offer effective tools, it also has to make sure people know how to use them. With this in mind, the social network has launched a new Safety Center that brings together a number of resources  for anyone to learn about online safety, on Twitter and beyond.  There are no new policies or tools here unfortunately, but the site explains in simple language what s tolerated, what isn t, and how users can better control their Twitter experience by muting, blocking, and reporting. The site does feel a bit cringingly earnest at times (sample text:  Twitter is a thrilling place for teens. ), but what educational resource doesn t?

For we-suck-at-dealing-with-abuse Twitter, any extra effort is welcome. Find out more at safety.twitter.com.

Learn how mute, block and report can help you take control of your experience on Twitter. https://t.co/nE1Qc45Xro

## Forget Phishing: Malware Now Coming for You Via Drones

The government may soon have a new way of getting spyware onto people’s computers: via drone.

Internal emails from the now infamous Hacking Team leak reveal that the company was in discussions with Boeing subsidiary Insitu to develop a way to infect computers via drone, according to a report from The Intercept.

Among the huge trove of data leaked by hackers earlier this month is a "roadmap" document with details about the projects on which Hacking Team’s engineers are currently working. One of the projects: To develop a small, rugged infection device that can be transported by drone.

According to The Intercept, the request "appears to have originated with a query from Washington-based Insitu"   aka, the same company that develops the ScanEagle surveillance drone, which is used by the U.S. military.

An Insitu engineer reportedly wrote to Hacking Team this April about the idea, stating: "We see potential in integrating your Wi-Fi hacking capability into an airborne system and would be interested in starting a conversation with one of your engineers to go over, in more depth, the payload capabilities including the detailed size, weight, and power specs of your Galileo System."

In a separate internal email, a Hacking team account manager suggested it can be done with a so-called "tactical network injector," or a portable device that can intercept a victim’s Internet traffic and secretly install spyware, according to The Intercept.

"Presumably, attaching a small network injector to a drone would give the ability to attack Wi-Fi networks from above, or at a greater distance," the report notes. "The system operator wouldn’t have to get physically near the target."

Insitu did not immediately respond to a request for comment.

## Microsoft Rushes Emergency Security Fix for Windows

Microsoft on Monday issued an emergency fix for all supported versions of its Windows operating system, plugging a hole that essentially allowed hackers unfettered access to victims’ computers.

The "critical" vulnerability, denoting Microsoft’s highest level of threat, would have allowed hackers to take "complete control of the affected system," the company wrote in an online security bulletin posted Monday. "An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights."

The flaw affects all users of Windows Vista, Windows 7, Windows 8 and 8.1 and Windows RT, representing two out of every three of the 1.5 billion PCs running Windows around the world. Microsoft decided not to wait until its regularly scheduled monthly security update, known as "Patch Tuesday," to issue a fix. The company last issued an emergency patch like this in November 2014.

Microsoft said a hacker could attack unsuspecting Windows users by convincing them to open a specially crafted document or visit a compromised Web page because the vulnerability affected OpenType, a widely used format for computer fonts co-developed by Microsoft and Adobe.

Computer security researchers found the flaw by looking over a collection of emails leaked online after cyberattackers breached the systems of Italian surveillance firm Hacking Team earlier this month. Microsoft credited security company FireEye’s Genwei Jiang and Mateusz Jurczyk, part of Google’s Project Zero security squad, for finding the flaw and reporting it.

The emergency fix comes at a sensitive time for Microsoft, which is just a week away from releasing the next big overhaul of its operating system, called Windows 10. Microsoft has touted the software upgrade as more secure than past versions of Windows. That’s thanks to new technology such as Device Guard, a software tool aimed at preventing the sort of attack today’s patch aims to avert, and Windows Hello, a new biometric security system that lets users add face, iris or fingerprint recognition to their computer for an added layer of protection.

Despite that, the security flaw patched today was found in even the latest test version of Windows 10, widely considered to be the final iteration of the software that will go out to the public and to device manufacturers.

Windows 10 will be available as a free upgrade for all Windows 7 and Windows 8.1 users on Wednesday, July 29.

Microsoft says a majority of Windows users have automatic updating enabled and will not need to make any extra effort to protect their machines. People who have have automatic updating turned off should download the patch from Microsoft’s security bulletin page.

The company says it has no evidence the flaw had been used to attack Windows, but confirmed such an attack could be exploited "consistently."

## Twitter Stock Pumped by Bogus Story About $31 Billion Buyout Offer

Fraudsters who posted a fake news story didn’t even bother to spellcheck the name of Twitter’s former CEO, but the story nonetheless briefly caused the company’s stock to spike.

The article, rigged to look like it came from Bloomberg, appeared online on Tuesday.

It claimed the company had received a $31 billion buyout order (about £19.8 billion).

Spokesmen for both Bloomberg and Twitter called the story fake.

The real Bloomberg reported that the US Securities and Exchange Commission (SEC) is looking into the possible pump-n-dump market manipulation.

Twitter’s stock rose by what Reuters said was more than 8.5% in the late morning.

According to Trade Alert data cited by Reuters, Twitter options were heavily traded on Tuesday with overall options activity surging to 330,000 contracts, or more than twice normal volume.

The price dropped after 20 minutes, but at close it was still trading 3% higher than it had the day before.

According to internet records, the bogus story site’s address was registered on Friday 10 July through a service in Panama that masks the identity of the owner.

The fake story was an artful counterfeit, possessing what the New York Times called a level of technical sophistication "rarely seen in such ruses."

For example, the article page, which closely resembled a standard Bloomberg report, contained multiple links that connected to real parts of Bloomberg’s website.

But as astute watchers noted - on Twitter, of course - there were some telltale giveaways.

For one thing, the story was headlined "Twitter Attracts Suitors" - a bit too fuzzy for the typically dry Bloomberg writing style, which would have been more likely to have run a title with wording along the lines of what Re/code suggested: "Twitter Is Said To Hire Advisors on Possible Sale."

Another bit of sloppiness was spelling former Twitter CEO Dick Costolo’s name wrong: the fraudsters spelled it "Costello."

Marc Andreessen ? @pmarca?Low IQ Tuesday! The fake Bloomberg story about Twitter being acquired couldn’t even bother to spell @dickc’s name right.

Of course, mistakes like these are handy ways to spot not only frauds meant to tinker with the stock market, but also the all too common cyber threat of phishing.

There are lots of things to watch out for besides orthographic (writing and spelling) mistakes when it comes to spotting fraud.

## Online Cheating Site AshleyMadison Hacked

Large caches of data stolen from online cheating site AshleyMadison.com have been posted online by an individual or group that claims to have completely compromised the company s user databases, financial records and other proprietary information. The still-unfolding leak could be quite damaging to some 37 million users of the hookup service, whose slogan is  Life is short. Have an affair.

The data released by the hacker or hackers   which self-identify as The Impact Team   includes sensitive internal data stolen from Avid Life Media (ALM), the Toronto-based firm that owns AshleyMadison as well as related hookup sites Cougar Life and Established Men.

Reached by KrebsOnSecurity late Sunday evening, ALM Chief Executive Noel Biderman confirmed the hack, and said the company was  working diligently and feverishly  to take down ALM s intellectual property. Indeed, in the short span of 30 minutes between that brief interview and the publication of this story, several of the Impact Team s Web links were no longer responding.

 We re not denying this happened,  Biderman said.  Like us or not, this is still a criminal act.

Besides snippets of account data apparently sampled at random from among some 40 million users across ALM s trio of properties, the hackers leaked maps of internal company servers, employee network account information, company bank account data and salary information.

The compromise comes less than two months after intruders stole and leaked online user data on millions of accounts from hookup site AdultFriendFinder.

In a long manifesto posted alongside the stolen ALM data, The Impact Team said it decided to publish the information in response to alleged lies ALM told its customers about a service that allows members to completely erase their profile information for a $19 fee.

According to the hackers, although the  full delete  feature that Ashley Madison advertises promises  removal of site usage history and personally identifiable information from the site,  users  purchase details including real name and address   aren t actually scrubbed.

 Full Delete netted ALM $1.7mm in revenue in 2014. It s also a complete lie,  the hacking group wrote.  Users almost always pay with credit card; their purchase details are not removed as promised, and include real name and address, which is of course the most important information the users want removed.

Their demands continue:

 Avid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers  secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails. The other websites may stay online.

It s unclear how much of the AshleyMadison user account data has been posted online. For now, it appears the hackers have published a relatively small percentage of AshleyMadison user account data and are planning to publish more for each day the company stays online.

 Too bad for those men, they re cheating dirtbags and deserve no such discretion,  the hackers continued.  Too bad for ALM, you promised secrecy but didn t deliver. We ve got the complete set of profiles in our DB dumps, and we ll release them soon if Ashley Madison stays online. And with over 37 million members, mostly from the US and Canada, a significant percentage of the population is about to have a very bad day, including many rich and powerful people.

ALM CEO Biderman declined to discuss specifics of the company s investigation, which he characterized as ongoing and fast-moving. But he did suggest that the incident may have been the work of someone who at least at one time had legitimate, inside access to the company s networks   perhaps a former employee or contractor.

 We re on the doorstep of [confirming] who we believe is the culprit, and unfortunately that may have triggered this mass publication,  Biderman said.  I ve got their profile right in front of me, all their work credentials. It was definitely a person here that was not an employee but certainly had touched our technical services.

As if to support this theory, the message left behind by the attackers gives something of a shout out to ALM s director of security.

 Our one apology is to Mark Steele (Director of Security),  the manifesto reads.  You did everything you could, but nothing you could have done could have stopped this.

Several of the leaked internal documents indicate ALM was hyper aware of the risks of a data breach. In a Microsoft Excel document that apparently served as a questionnaire for employees about challenges and risks facing the company, employees were asked  In what area would you hate to see something go wrong?

Trevor Stokes, ALM s chief technology officer, put his worst fears on the table:  Security,  he wrote.  I would hate to see our systems hacked and/or the leak of personal information.

In the wake of the AdultFriendFinder breach, many wondered whether AshleyMadison would be next. As the Wall Street Journal noted in a May 2015 brief titled  Risky Business for AshleyMadison.com,  the company had voiced plans for an initial public offering in London later this year with the hope of raising as much as $200 million.

 Given the breach at AdultFriendFinder, investors will have to think of hack attacks as a risk factor,  the WSJ wrote.  And given its business s reliance on confidentiality, prospective AshleyMadison investors should hope it has sufficiently, er, girded its loins.

Update, 8:58 a.m. ET: ALM has released the following statement about this attack:

 We were recently made aware of an attempt by an unauthorized party to gain access to our systems. We immediately launched a thorough investigation utilizing leading forensics experts and other security professionals to determine the origin, nature, and scope of this incident.

 We apologize for this unprovoked and criminal intrusion into our customers  information. The current business world has proven to be one in which no company s online assets are safe from cyber-vandalism, with Avid Life Media being only the latest among many companies to have been attacked, despite investing in the latest privacy and security technologies.

 We have always had the confidentiality of our customers  information foremost in our minds, and have had stringent security measures in place, including working with leading IT vendors from around the world. As other companies have experienced, these security measures have unfortunately not prevented this attack to our system.

 At this time, we have been able to secure our sites, and close the unauthorized access points. We are working with law enforcement agencies, which are investigating this criminal act. Any and all parties responsible for this act of cyber terrorism will be held responsible.

 Avid Life Media has the utmost confidence in its business, and with the support of leading experts in IT security, including Joel Eriksson, CTO, Cycura, we will continue to be a leader in the services we provide.  I have worked with leading companies around the world to secure their businesses. I have no doubt, based on the work I and my company are doing, Avid Life Media will continue to be a strong, secure business, Eriksson said.

## Windows XP Anti-Malware Support Terminated   180 Million Users Left Vulnerable

Millions of Windows XP users are now left vulnerable to malware attacks as Microsoft has decided to terminate support and security updates for Microsoft Security Essentials package for Windows XP.

For those of you who don t know, Microsoft announced more than a year ago, on the 8th of April 2014 that the support for Windows XP s security update has been officially ended, this means all those users who are running Windows XP on their systems are vulnerable because the potential security weaknesses are not being patched.

On the other hand, Microsoft Security Essentials, a free antivirus solution by Microsoft, continued to receive constant security and antimalware signature updates because of the peer pressure from the corporate companies and users who were still planning to upgrade their systems to an advanced and secure operating system.

But then again, on July 14th 2015, the company decided to officially end the support for their antivirus and antimalware software i.e. Microsoft Security Essentials (MSE) as well as the Malicious Software Removal Tool (MSRT). From this point forward, there won t be any updates and support for Windows XP.

For those who are still running Windows XP on their systems, Microsoft said:

If you continue to use Windows XP now that support has ended, your computer will still work but it might become more vulnerable to security risks and viruses. Internet Explorer 8 is also no longer supported, so if your Windows XP PC is connected to the Internet and you use Internet Explorer 8 to surf the web, you might be exposing your PC to additional threats. Also, as more software and hardware manufacturers continue to optimize for more recent versions of Windows, you can expect to encounter more apps and devices that do not work with Windows XP.

While warning the Windows XP users, Microsoft said that the Windows will continue to operate and run on your system but running an unsupported version of operating system can be very risky because:

An unsupported version of Windows will no longer receive software updates from Windows Update. These include security updates that can help protect your PC from harmful viruses, spyware, and other malicious software, which can steal your personal information.

Security of OS is one of the most crucial part but, according to the statistic and report published by Andra Zaharia of Heimdal Security, this unfriendly move by Microsoft has leftover 12 percent or 180 million users without any security, making them more vulnerable to persistent spyware and malware attacks.

Nevertheless, Windows XP users can still install third-party antimalware solutions on their systems to protect themselves from the potential vulnerabilities, but the company advised that all those computer systems running this specific version of operating system will remain unprotected due to unpatched security loopholes.

Microsoft said in their antimalware support document for Windows XP:

While the anti-malware updates enable the ability to detect and block certain malware on Windows XP PCs, it is important to note that since the underlying vulnerability in the Windows XP operating system will not be patched with a new security update, a new strain of malware attacking the same vulnerability may not be detected in the future and may be able to infect the PC.

Microsoft is trying their best to cut down the overall market share of Windows XP by forcing users to move to the latest and much-advanced OS like Windows 8.1 and Windows 10. Though, there is a large number of users who are still running Windows XP because upgrading would require them to invest into new hardware too.

## Self-Destructing Gmail Possible With Free Chrome Extension

That drunk email sent to an ex-boyfriend can now easily be revoked with the click of a button.

A new Chrome extension called Dmail brings its self-destructing super powers to a user’s Gmail inbox, allowing users to take control of the messages they send even long after they’ve been fired off to the recipient.

Email panic or regret can be fixed by clicking the "revoke" button after a message has been sent. When sending a message, users can also decide whether they want the message to self-destruct after one hour, one day, one week or never.

Messages sent to a friend who has Dmail appear in their inbox as normal. The extension still works if a friend doesn’t have the service. They’ll instead be given a Dmail link in the email which will take them to the secure message.

The extension was developed by the team behind the Delicious social bookmarking tool. The group noted on their company blog that while they’re still early in the product process "but we built this tool out of a pain many of us have experienced and we hope it makes life easier for you as well."

Google unveiled its "undo send" feature in June giving Gmail users with email panic or regret up to 30 seconds to take back the offending message. The feature was first launched in Google Labs in 2009.

If the sender doesn’t cancel during their email grace period, the message will be sent to the recipient as soon as the delay expires. Using the feature requires users to opt into the service by visiting their Gmail settings section.

# Patch Tuesday: Not Dead Yet

Patch Tuesday is not dead.

That’s what experts have now concluded, even though Microsoft will not say straight out if it plans on upending the 12-year practice of providing security patches on the same day each month to everyone.

With Windows 10’s launch only five days away - the new operating system will debut July 29 on previewers’ PCs - the question of whether Patch Tuesday lives and breathes, or will die a sure death, maybe quickly, maybe slowly, still remains officially unanswered.

But security professionals and industry analysts have come to the conclusion that Patch Tuesday will continue, possibly in the same form it has since 2003.

"Patch Tuesday is not going away any time soon," said Chris Goettl, product manager for patch management vendor Shavlik. "It’s been blown out of proportion."

"Patch Tuesday" is the label that’s been stuck to the second Tuesday of each month, the day Microsoft has issued its security updates since 2003. (Microsoft prefers the more upbeat "Update Tuesday.") The practice was begun to make patching more predictable, especially for businesses - the Redmond, Wash. company’s biggest and best customers - who generate the bulk of the firm’s revenue.

Two months ago, Patch Tuesday’s survivability seemed in doubt after Windows chief Terry Myerson said, "We’re not going to be delivering all of the updates to all of these consumers on one day of the month," when talking about changes to Windows Update under Windows 10.

Observers used that comment to conclude that Microsoft was killing Patch Tuesday and would instead roll out security fixes as soon as they were ready, returning to its pre-2003 practice. Two weeks ago, when Microsoft shipped its July batch, some marked it as the last-ever Patch Tuesday.

Hold the phone, security experts said. While they agreed that Patch Tuesday would be moot for consumers on Windows 10, even in May they were certain it would remain a factor for businesses, although fixes would be available as they exited Microsoft’s testing.

Microsoft hasn’t been any help. This week, it again declined to answer questions about when and how security updates would be distributed to Windows 10 devices.

When asked whether security updates would be offered to all Windows 10 users on the second Tuesday of each month, or issued to all users as the fixes are completed and approved by Microsoft, a spokesman would not address the question. Instead, he said, "With Windows 10, we will deliver ongoing innovations and security updates. Frequency and delivery of updates may vary based upon the update."

That varied delivery he mentioned would not be any different than the company’s current policy, which at times steps outside the Patch Tuesday schedule to ship rush fixes, or so-called "out-of-bound" updates. It did that just this week when it released an emergency update to all Windows editions.

Asked whether security updates would be packaged within Windows 10’s expected regular tempo of feature and functionality updates - as was an emergency Windows 10 patch distributed July 15 and several more since then - and released to users via the OS’s multiple cadences, dubbed "branches" and "rings," the spokesman declined to comment. "Microsoft has nothing to share on that at this time," the spokesman said in an email, using one of the company’s standard lines.

Two months ago, some security pros criticized Microsoft for not being more forthcoming. "Microsoft’s communications have gone to near zero," said Andrew Storms, vice president of security services at consultancy New Context, in a May interview. "To some degree, that’s part of the reason why everyone is confused."

Microsoft’s reticence may have exacerbated the confusion, but it largely stemmed from the radical overhaul of the Windows update, upgrade and servicing model. Rather than ploddingly roll out a new OS every three years, Microsoft will continually deliver new tools and functionality, new user interface (UI) and user experience (UX) features and enhancements over the life of Windows 10.

Microsoft has long updated Windows on a regular basis, but only in the form of security patches and bug fixes. They will now be accompanied by more visible improvements. But how the two categories - in Microsoft’s parlance, "non-security" and "security" updates, the former encompassing everything but patches - interact, intersect and overlap, or even if they do at all, is the foundation of the mystery.

Because Microsoft has been feeding off-the-cuff security updates that also include non-security content to Windows Insiders - the people who have opted in to the Windows 10 preview program - many have concluded that that will be the norm for everyone, or at the least, consumers on the "Current Branch" (CB), the earliest-to-get-updates mainstream track that’s the only one available to customers running Windows 10 Home.

"That’s the only cadence that people are seeing right now," Goettl pointed out.

But there’s no guarantee that how Microsoft ships security updates to the Insider group will be the way it treats the Current Branch. Gabriel Aul, engineering general manager for Microsoft’s OS group, hinted at that possibility Tuesday. "The experience you’re having is because you’re in the Insider program. Not how the rest of the world will experience," Aul tweeted when a user griped about the barrage of updates to Insider build 10240.

Even with the muddy waters, Goettl remained convinced that consumers would no longer see Patch Tuesday, at least as it’s been known in the past. "Consumers will get things as they come out," he said today, reiterating his position of May. "They’ll have little choice on it, but that’s okay. Consumers have the least knowledge [about patches] and they shouldn’t be making the decision. Windows 10 will be like the Apple model [for Macs], and that’s in [consumers’] best interest."

Again, Microsoft has not said as much. Nor has the company laid out how security updates will be presented to businesses. But there, people like Goettl and others were surer of what will happen.

Businesses that rely on the "Current Branch for Business" (CBB) and/or "Long-term Servicing Branch" (LTSB) for non-security updates will continue to see a Patch Tuesday, Goettl asserted. In fact, he argued that it was this critical part of Microsoft’s customer mix that’s calling the shots. "They have forced the course on Patch Tuesday," Goettl said.

Gartner’s analysts were more aggressive in their belief that Patch Tuesday would remain intact, saying that it would exist for consumer and commercial Windows users. "[Current Branch] does not replace the current monthly security patch program, which will continue to deliver critical security fixes on the second Tuesday of each month," wrote Gartner analyst Steve Kleynhans in a recent report for clients. "Security fixes will continue to arrive each month on Patch Tuesday regardless of which branch you select, although they may arrive even more frequently for those on Windows Update."

In a follow-up email, Kleynhans said that although Gartner had no inside information, it expects Patch Tuesday to continue.

But Kleynhans, like everyone else, will just have to wait for Microsoft to say how it is. Or isn’t.

## Microsoft: Here’s Why You Should Upgrade to Windows 10

Microsoft has kicked off a new series of videos and blog posts that aim to explain why you should upgrade to Windows 10.

Launched on Sunday, the initial blog post authored by the Windows Team focuses on the Start menu, which is alive and well once again in Windows 10 but with a few twists. The team highlights the new Start menu by saying it’s back in a "more robust and expanded format" with access to your most frequently used apps, Windows settings and space to add live tiles.

Following the feeble response to Windows 8, Microsoft needs Windows 10 to be a hit. As such, the company has been fine-tuning its new OS since October 2014 with ongoing new versions, or builds, of its current Technical Preview based in part on user feedback. One way Microsoft has been enhancing Windows 10 is by bringing back some of the features from Windows 7 that people have missed. And Numero Uno on the list is the Start menu. Even Microsoft now realizes it made a major boo boo by killing the Start menu in Windows 8 in favor of the Start screen. People don’t like change. And the Start menu was a familiar way of working. Now in Windows 10, the Start menu has returned, but with some of the Windows 8 flair.

So what goodies will you find in the new Start menu that Microsoft thinks you’ll love?

The apps you use most most frequently automatically show up on the menu. Windows 7 has a similar effect. The menu also offers a spot to discover newly-installed apps as well as suggested apps based on the software you currently run. A section called Places provides quick access to File Explorer for managing your files, the Power button for shutting down or restarting Windows and the Settings command for tweaking your Windows options.

Perhaps what’s most different in the new Start menu is that it incorporates the tiles from the Windows Start screen. So you can pin your favorite Windows apps to the right pane of the Start menu and view live tiles for News, Weather and other apps that show you up-to-the minute information. With the new menu, Microsoft is blending elements of Windows 7 and Windows 8.1, an approach designed to appeal to people who like the traditional menu as well as those who prefer the Start screen.

In its blog, the Windows Team also attempts to reassure Windows 7 and 8.1 users concerned about upgrading to Windows 10 that they’re in good hands.

"Over 5 million Windows Insiders have been helping us test Windows 10 and make it our best Windows ever," the team said. "They’re also helping us make the upgrade process smooth and easy. Upgrade preserves your documents and files so you don’t need to worry about things getting lost. Plus you can pick up the phone or text chat with the Microsoft Answer Desk for any reason. It’s all part of our ’No worries’ approach."

Known as "10 Reasons to Upgrade," the video hosted on the blog is a quickie, running just 45 seconds. But it says a lot in that short time. In touting the return of the Start menu and the integration with live tiles, Microsoft sees Windows 10 as something familiar, offering the best of Windows 7 and the best of Windows 8. And it clearly wants users to see it the same way.

The team urges people to stay tuned for more blog posts leading up to the July 29 launch of Windows 10. Other features the team will be touting include the Cortana voice assistant, the new Edge browser, the Xbox app, and the Windows Hello biometric security that lets you log in using your face or finger.

## 8 Reasons Not to Upgrade to Windows 10

After months of hype and media attention, Windows 10 is almost here. That means it s decision time: Do you upgrade as soon as you can? Or do you wait?

Hard as it may be to resist the immediate promise of a better computing experience, upgrading to a new operating system as soon as it s available isn t always the best idea. Why? Glad you asked. Here are eight reasons you might want to consider not upgrading to Windows 10.

### If it ain t broke

Sure, Windows 10 will be a free upgrade for current Windows users. But price isn t the only thing you should consider when deciding to upgrade or not. The real question is, What are you going to get? Sure, there s some fancy new touch interaction and a personal assistant you can talk to   cool story, Microsoft. But  cool  doesn t always equal  compelling.

If you re happy with your current Windows 7 or 8 setup, why change it? Remember, Microsoft has promised to keep supporting Windows 7 until 2020, Windows 8 until 2023. And you ve got a year to take advantage of the free upgrade offer. Why the rush?

Unless you have some serious tech-savvy, downgrading from Windows 10 to a previous version is going to be a serious undertaking. And there s always the chance that you ll lose apps and/or data during that downgrade process.

Point being, once you hit that upgrade button, it s going to be really tough to go back, should you have second thoughts. Why not wait until you re absolutely certain you re ready for the new OS?

Microsoft can scream all it wants about shiny new features in Windows 10. But with a little patience and a few Web searches, you can get many of those  new  features now by tweaking your older version of Windows.

For example, Windows 10 brings back the Start menu. But our very own David Pogue showed you how to get that menu in Windows 8 (or 8.1) last year. The shiny new Edge browser looks cool and all, but it doesn t do a whole lot that Chrome or Firefox   with the appropriate settings and extensions can t.

Despite Microsoft s best efforts at collecting feedback from early adopters through its extensive Windows 10 technical preview process, bugs and other issues are still going to surface in the launch-day version of the new OS.

Let others be the guinea pigs, and wait until the bugs are ironed out. You ll thank yourself in the long run.

Microsoft is taking a proactive approach by requiring all Windows 10 Home users to accept forced updates and reinstalls of the core apps.

This lack of control leaves you at the mercy of Microsoft, regardless of how you feel about new apps or redesigned interfaces. Should Microsoft push an update that breaks your system   well, too bad.

Windows 10 completely does away with Windows Media Center. According to Microsoft, once you upgrade to Windows 10, WMC will all but disappear, leaving you to figure out some other means of accessing your entertainment content.

So don t upgrade to Windows 10 if you rely on and use Windows Media Center on a daily basis.

Regardless of how long third-party developers have had access to Windows 10 to test their code against, it won t be enough for all of them. If you rely on a given app to do your job, check with its developer about its Windows 10 compatibility before you click on that install button.

Microsoft has laid out some minimum hardware requirements for PCs to run Windows 10. But let s be honest: Just because your PC meets those requirements, that doesn t necessarily mean you ll be happy with the results.

If you find yourself with an older computer that s on the bubble between compatible and not, and that PC runs your current OS just fine, you can wait until you upgrade your computer before you update Windows.

## Like It Or Not... You Can’t Disable Windows 10 Automatic Updates

Windows 10 is all set to launch on July 29 and will also be available on USB drives for purchase in retail channels.

So, if you are planning to install Windows 10 Home, one thing you must keep in your mind   You wish or not, the software updates for Microsoft s new operating system will be mandatory.

Microsoft is planning to make a significant change to its software update policy by "removing the option to DISABLE software updates in Windows 10 Home".

This clearly indicates that all users of Windows operating system must agree to allow Microsoft to install software updates automatically.

In Windows 8.1, users get four options for Windows Update's behavior, which include:

Download and Install Windows Updates Automatically
Download Windows Updates automatically but Choose when to Install them
Check for Updates but Choose when to Download and Install them
Never check for, Download, or Install Updates

From a Security point of view, the last option, i.e. never to download or install updates, is not at all recommended by either the company or the security experts. However, the option is still there if Windows users really need it.

In Windows 10, the options for Windows Update are cut to only two, which include:

Check, Download, Install, and Reboot automatically
Check, Download, Install automatically and then choose to Reboot

Here is the EULA to which you agree to when you accept the terms of the licensing agreement:

"Updates. The software periodically checks for system and app updates, and downloads and installs them for you. You may obtain updates only from Microsoft or authorized sources, and Microsoft may need to update your system to provide you with those updates. By accepting this agreement, you agree to receive these types of automatic updates without any additional notice."

If this happens with the launch of Windows 10, it would be a notable change in any version of Windows OS as Microsoft has talked about Windows 10's Windows-as-a-Service approach that will receive continuous updates.

Every software program needs frequent updates, but the ability of Windows users to permanently delay Windows software updates has made it difficult for Microsoft to keep its OS platform secure and up-to-date. And the only motive behind this change is to maintain the security of its users safety.

=~=~=~=

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.